UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

JOLYNNE CHRISTIANSEN; JOHN DOE; EVELYN HARRIS; DANIEL MCCORMICK; JOAN MIGLIACCIO; MICHELLE MULANAX; KELLY ROSAL, GARY ROWE, and DAVID YANCEY, ***individually and on behalf of all others similarly situated,*** **Plaintiffs,** **v.** **PARKER HANNIFIN CORPORATION,** **Defendant.**	**Lead Case No. 1:22-cv-835** **Consolidated with:** **Case No.: 1:22-CV-00852;** **Case No.: 1:22-CV-00891;** **Case No.: 1-22-CV-00943;** **Case No.: 1:22-CV-01073;** **Case No.: 1:22-CV-01229.** **Judge Hon. Dan Aaron Polster** **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Jolynne Christiansen, John Doe, Evelyn Harris, Daniel McCormick, Joan Migliaccio, Michelle Mulanax, Kelly Rosal, Gary Rowe, and David Yancey (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this Consolidated Class Action Complaint ("Complaint" or "Consolidated Action") against Defendant Parker Hannifin Corporation ("Parker" or "Defendant"), an Ohio corporation, to obtain damages, restitution, and injunctive relief. Plaintiffs make the following allegations upon information and belief, their own personal knowledge, the investigation of counsel, and the facts that are a matter of public record.

INTRODUCTION

1. Conti is a well-known ransomware group that has attacked more than 400 organizations worldwide (including more than 290 in the United States) over the span of more than

a year. It generally uses the same modus operandi, hacking and exfiltrating sensitive data of an organization and then holding it for ransom. The FBI and others have issued warnings and advisories—advisories that provide detailed instructions for how to avoid a Conti attack. Widely available software has been developed that protects against Conti attacks.

2. Parker did not protect itself from this known threat. In fact, it not only failed to meet regulatory and industry standards for cybersecurity, but also failed to take the most basic security measures such as encryption of data and destruction of obsolete data. As a result, between March 11-14, 2022, Conti gained access to the sensitive and personal information (including, for example, Social Security numbers and the even more valuable to Conti medical information) of more than 120,000 of Parker's and its subsidiaries' current and former employees and their dependents ("Class Members"). This information went back decades.

3. Conti accessed and exfiltrated the information, holding it for ransom. Conti initially posted a small amount of this information on the internet to demonstrate that it actually had the data and then, apparently when Parker refused to pay a ransom, Conti posted the rest on the internet on April 20, 2022. The website page containing the information has been accessed over 17,000 times.

4. While the breach occurred between March 11-14, 2022, Parker did not detect suspicious activity until March 14, 2022. Conti took public credit for the breach on April 1, 2022. But it was not until May 10, 2022 that Parker began notifying the affected people that their sensitive information had been taken. No reason was given for the delay.

5. The data breach has caused damage. Plaintiffs have already spent a great deal of time attempting to mitigate the damage caused, and have suffered damages from misuse of the data taken. Plaintiff Jolynne Christiansen was notified by her credit card company that her account

had been compromised. Plaintiff John Doe received notification that his personal information had been exposed on the internet at least twenty-six times. Plaintiff Daniel McCormick received notification that he was a victim of identity theft in June 2022. And the threat of continued misuse is not only present and imminent, but will last for years.

NATURE OF THE ACTION

6. This Consolidated Action arises out of the above-described data breach ("Data Breach") involving Defendant, a multibillion-dollar manufacturing company headquartered in Cleveland, Ohio. The specific types of data accessed, acquired, stolen, disseminated, and published in the Data Breach included Plaintiffs' and Class Members' full names, Social Security numbers, dates of birth, addresses, driver's license numbers, U.S. passport numbers, financial account information (bank account and routing numbers), online account usernames, and passwords (collectively, "PII"). The Data Breach also included protected health information such as health insurance plan member ID numbers and dates of coverage (collectively, "PHI") (PII and PHI are referred to collectively as "Private Information").

7. Plaintiffs and Class Members include current and former employees of Defendant and its acquired entities, their dependents, and other individuals affiliated with Defendant whose Private Information was compromised in the Data Breach.

8. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and will suffer additional injuries into the future. Plaintiffs are making claims for damages and remedies for the following categories of harms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in

Defendant's notice letter ("Notice Letter"); (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring for the Class; (g) loss of time incurred due to actual identity theft; (h) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; (i) deprivation of value of their PII; and (j) statutory damages.

9. Plaintiffs and Class Members are also seeking injunctive relief for the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the Private Information.

10. Accordingly, Plaintiffs, on behalf of themselves and other members of the Classes (as defined *infra*), assert claims for (i) negligence; (ii) negligence *per se*; (iii) breach of implied contract; (iv) unjust enrichment; (v) declaratory relief; (vi) violations of the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100 *et seq.*; (vii) violations of the Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56 *et seq.*; (viii) invasion of privacy under the California Constitution, Article I, Section 1; (ix) violations of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*; and (x) violations of the New York General Business Law § 349. Plaintiffs seek injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiffs

11. Plaintiff Jolynne Christiansen is a natural person and a resident and citizen of Minnesota. Plaintiff is a former employee of Defendant, where she worked for approximately one year in the late 1980s or early 1990s. Defendant notified Plaintiff Christiansen of the Data Breach and unauthorized access of her Private Information by sending her a Data Breach Notice Letter, dated May 10, 2022.

12. Plaintiff John Doe[1] is a natural person and a resident and citizen of California. Plaintiff Doe was an employee of Defendant from approximately June 2018 through August 2019. Defendant notified Plaintiff Doe of the Data Breach and unauthorized access of his Private Information by sending him a Data Breach Notice Letter, dated May 10, 2022.

13. Plaintiff Evelyn Harris is a natural person and a resident and citizen of Ohio. Plaintiff Harris was an employee of Defendant from approximately 1976 through April 2019. Defendant notified Plaintiff Harris of the Data Breach and unauthorized access of her Private Information by sending her a Data Breach Notice Letter, dated May 10, 2022.

14. Plaintiff Daniel McCormick is a natural person and a resident and citizen of California. Plaintiff McCormick was an employee of Defendant from 2010 through 2011. Defendant notified Plaintiff McCormick of the Data Breach and unauthorized access of his Private Information by sending him a Data Breach Notice Letter, dated May 10, 2022.

15. Plaintiff Joan Migliaccio is a natural person and a citizen and resident of New York. Ms. Migliaccio was a dependent of a former employee of Parker, and her Private Information was provided to Parker as a condition of her husband's employment. Defendant notified Plaintiff Migliaccio of the Data Breach and unauthorized access of her Private Information by sending her a Data Breach Notice Letter, dated May 10, 2022.

16. Plaintiff Michelle Mulanax is a natural person and a citizen and resident of Ohio. Plaintiff Mulanax is a former employee of Defendant who provided her Private Information to Defendant as a condition of her employment. Defendant notified Plaintiff Mulanax of the Data

[1] Due to the sensitive nature of this action and the fact his information appears to be available on the dark web, Plaintiff has elected to file under a pseudonym. *See, e.g., Doe v. Kaweah Delta Hosp.*, 2010 U.S. Dist. LEXIS 135808 (E.D. Cal., Dec. 22, 2010); *Does I thru XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1067 (9th Cir. 2000).

Breach and unauthorized access of her Private Information by sending her a Data Breach Notice Letter, dated May 10, 2022.

17. Plaintiff Kelly Rosal is a natural person and a citizen and resident of Wisconsin. Plaintiff Rosal was an employee of Defendant from approximately 2001 through 2015. Defendant notified Plaintiff Rosal of the Data Breach and unauthorized access of his Private Information by sending him a Data Breach Notice Letter, dated May 10, 2022.

18. Plaintiff Gary Rowe is a natural person and a resident and citizen of Connecticut. Plaintiff Rowe is a former employee of Defendant from approximately 1979 until 1999. Defendant notified Plaintiff Rowe of the Data Breach and unauthorized access of his Private Information by sending him a Data Breach Notice Letter, dated May 10, 2022.

19. Plaintiff David Yancey is a natural person and resident and citizen of the State of North Carolina. Defendant notified Plaintiff Yancey of the Data Breach and unauthorized access of his Private Information by sending him a Data Breach Notice Letter, dated May 10, 2022.

Defendant Parker Hannifin

20. Defendant is a global corporation incorporated in the State of Ohio with its principal place of business in Cleveland, Ohio (Cuyahoga County). Parker has approximately 13,000 locations globally, and for more than 100 years has provided engineering services and specialized products to industrial and aerospace markets. Service of Process is proper on Nicholas Strieker at 4495 W. 140th St., Cleveland, Ohio 44135.

JURISDICTION & VENUE

21. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the

proposed Class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

22. The Northern District of Ohio has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Ohio and this District through its headquarters, offices, parents, and affiliates.

23. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Background

24. Defendant is a Fortune 250 engineering company specializing in motion and control technologies, with corporate headquarters in Mayfield Heights, Ohio, in Greater Cleveland. The company provides precision engineered solutions for organizations in the aerospace, mobile, and industrial sectors. It has thousands of employees and operates globally.

25. In applying for jobs and/or accepting employment with Defendant or its subsidiaries, Plaintiffs and many Class Members were required to provide Defendant with sensitive and confidential information, including their names, dates of birth, and Social Security numbers, which is static information that does not change and can be used to commit myriad financial crimes as well as identity theft. Applicants must also provide additional information, including but not limited to health information, financial account information, and government issued identification numbers such as passport numbers.

26. Plaintiffs and Class Members relied on Defendant (a large, sophisticated entity) to

keep their Private Information confidential and securely maintained, to use this information for business purposes only, to make only authorized disclosures of this information, and to implement and follow adequate and reasonable data retention policies. Defendant maintained and stored the Private Information on its systems and networks that were ultimately accessed in the Data Breach.

27. Defendant owed Plaintiffs and Class Members numerous statutory, regulatory, contractual, and common law duties to safeguard and keep Plaintiffs' and Class Members' Private Information confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, and theft.

28. Defendant also recognized its responsibility and voluntarily adopted policies and procedures to protect Private Information in its Personal Data Privacy Policy ("Privacy Policy"). The Privacy Policy is publicly posted to the internet and is provided to its employees.[2]

29. The purpose of this policy is to "inform employees and third parties with whom Parker has a business relationship of the principles under which Parker collects, uses, transfers and retains Personal Data" and it "applies to all Personal Data received or collected by Parker."[3]

30. The Privacy Policy includes the following representations:

> Only the Personal Data that is necessary for a legitimate business reason or as required by applicable laws or regulations (the "Purpose") should be collected and Processed. When the Purpose for the Personal Data has ended or is no longer relevant, the Personal Data should be deleted, taking into consideration the relevant Records Retention and Protection Guidelines (1.04). Any retention of Personal Data beyond the relevant time period set forth in the Records Retention and Protection Guidelines (1.04) must be documented and explicitly state the reasoning for such retention beyond the specified period.
> …
> Parker collects and uses Personal Data for the purposes of management and administration of its pre-employment, employment, and post-employment relationships. The Personal Data is collected and used for hiring activities, general workforce management (described

[2] *See* https://www.parker.com/portal/site/PARKER/menuitem.4450f18f18c082cdfd40eae8237ad1ca/?vgnextoid=cb333a5693983610VgnVCM100000e6651dacRCRD (last visited May 19, 2022).
[3] *Id.*

> further below), administering security at Parker facilities and on Parker information systems, and as necessary to maintain Parker's third party relationships with customers, suppliers, and other third parties. General workforce management includes, for example, time and attendance tracking, payroll, brokering, providing and administering services and other benefits to employees and their dependents and beneficiaries, job performance and talent management, production of company address books and directories, management of communication systems, training and employee development, providing and monitoring the use of company resources such as company vehicles, mobile phones, computers, and travel and mobility services, managing emergency contact details, and meeting governmental reporting requirements.
> …
> Parker also may transfer Personal Data between countries, including but not limited to Parker's global headquarters located in the United States of America. Parker is committed to protecting the privacy and confidentiality of Personal Data when it is transferred and employs adequate safeguards and protections in any such transfer, including compliance with the EU-US (and the Swiss-US) Privacy Shield Framework.
> …
> Parker takes reasonable precautions to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. These precautions include, for example, password protections for online information systems, restricting access to Personal Data, and employing electronic security measures to protect against hacking or other unauthorized access. Additionally, Parker provides physical security to prevent unauthorized access to database equipment or hard copies of Personal Data.

The Data Breach

31. On March 14, 2022, Defendant detected suspicious activity on its network.

32. Between March 11-14, 2022, a third party gained unauthorized access to Defendant's computer systems and exfiltrated 419GB worth of documents containing the sensitive information of its current and former employees (as well as their dependents).[4]

33. On April 1, 2022, a well-known ransomware group named Conti took credit for the Data Breach and posted a 5GB sample of stolen data to the internet.

34. On or about May 12, 2022, Defendant reported a data breach affecting almost 120,000 current and former employees, their dependents, and others, both of Defendant and

[4] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/amp/ (last visited May 19, 2022).

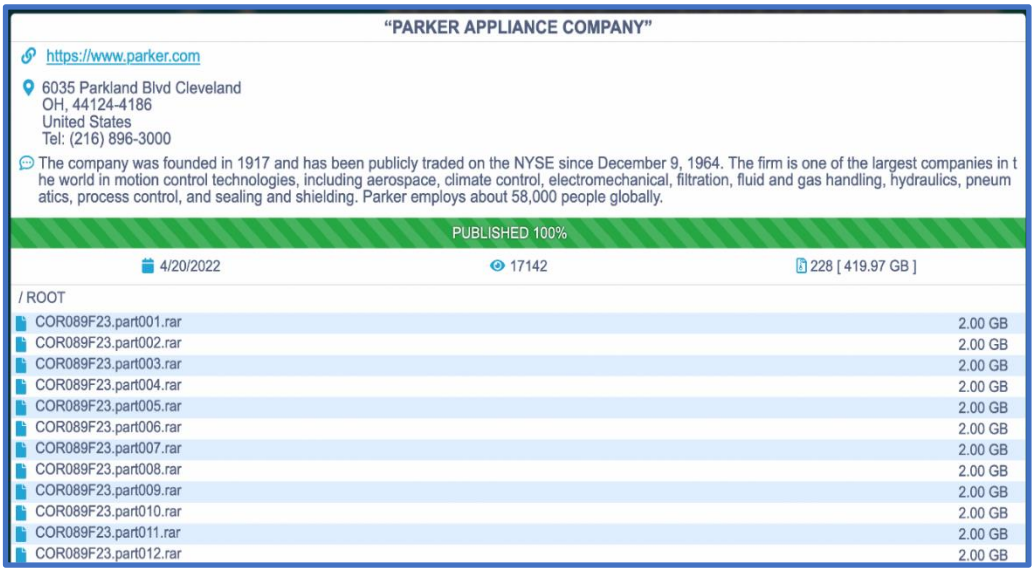
numerous subsidiaries.

35. In addition, current or former enrollees of Defendant's Group Health Plan overseen by the Parker Benefits Service Center (or a health plan sponsored by an entity acquired by Defendant), may also have been subject to unauthorized access and theft.

36. Defendant's public statement about this data breach and ransomware attack was first disclosed in a Form 8-K filed with the Securities and Exchange Commission on or about April 5, 2022, which stated that "a third party gained unauthorized access to the Company's systems" from March 11-14, 2022. Defendant's filing also stated that "the Company believes some data was accessed and taken and may include personal information of Company team members." Defendant did not begin notifying affected individuals until on or about May 13, 2022, two months after the Data Breach.

37. While not included in Defendant's public statements about this incident, Security Week reports that Parker's attack was perpetrated by the Conti ransomware group. On or about April 1, 2022 the Conti group published 5 GB of the stolen files on the internet, which purportedly was only 3% of the data taken.

38. This sort of publication is initially done to prove the personal data has been successfully stolen.



(*screenshot of the Conti data leak page for PARKER-HANNIFIN as of May 19, 2022)*

39. On or about April 20, 2022, Conti announced through its data leak page that 100% of the data taken from Defendant has been published. The size of the data purportedly released to the internet for open access is 419.97 GB. It further appears that this data leak page has been publicly viewed and accessed over 17,000 times.

40. Conti demanded that Defendant pay a ransom for the safe return and deletion of the Private Information stolen from it. Defendant apparently refused this demand.

41. Upon information and belief, the Conti ransomware group accessed and exfiltrated this data with the intent to misuse it, including to demand ransom, marketing and/or selling this information on the internet.

42. Despite the incredible risk faced by Plaintiff and Class Members, Defendant waited until May 12, 2022 to begin mailing notification letters to the victims of the Data Breach ("Notice Letter").[5]

[5] A copy of the template notice letter is available online through the California Attorney General: https://oag.ca.gov/system/files/Parker%20Hannifin%20-%20California%20Notification.pdf (last visited on July 13, 2022); Furthermore, Defendant posted about the Data Breach on its website:

43. Defendant's Notice Letter to victims of the Data Breach reprehensibly downplayed the risk victims face by failing to mention that their most sensitive Private Information had already been published to the internet. Defendant's Notice Letter only that stated an unauthorized person had gained access to its IT servers. To date, Defendant has never disclosed that it was the subject of a ransomware attack, that its systems had been copied and exfiltrated by the Conti ransomware group, whether or not Defendant paid the ransom, and that all of this Private Information had been stolen and was disclosed on the internet.

44. Presaging the harm that Defendant knew would impact victims of its Data Breach, the Notice Letter advised Plaintiffs and Class Members "to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity." Defendant also offered the Plaintiffs and Class Members a two-year membership in Experian's Identity Works to help "detect possible misuse of your information" and provide "identity theft protection."

45. Currently, the full extent of the types of sensitive personal information, the scope of the Data Breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation. However, Plaintiffs and Class Members are aware that the type of data set published now provides a one-stop shop for identity thieves to wreak complete havoc on their lives. Given the sensitivity and static nature of the information involved (such as names, Social Security numbers, and dates of birth), and the criminal targeting, theft and publication of the data on the internet, Plaintiffs and Class Members have all experienced a materialized and imminent risk of identity theft.

---

https://www.parker.com/parkerimages/Parker.com/Countries-2011/United%20States/Web_Posting_Final.png (last visited on July 13, 2022).

46. Cybersecurity experts who have reviewed this matter have specifically concluded that the information taken in the Data Breach "would make it possible for malicious actors to carry out phishing attacks, social engineering, or even identity theft and bank fraud."[6]

47. Incredibly, the Private Information that Conti exfiltrated in the Data Breach was held in unencrypted form by Defendant, and included former employees' and their dependents' Private Information that Defendant had continued to possess for many years (including up to several decades for some Class Members) without any legitimate business purpose. There is no reasonable justification for Defendant to retain Plaintiffs' and Class Members' Private Information in unencrypted form for such long periods of time.

48. On May 13, 2022, the U.S. Department of Health and Human Services Office for Civil Rights ("HHS OCR") was notified that the Data Breach included the Private Information of 119,513 current and former employees.[7] The number of victims is likely greater than this, as it has been reported that the number publicly posted on the HHS OCR website only includes individuals currently or formerly enrolled in the Parker Group Health Plan.[8]

49. Defendant has tacitly admitted that the Private Information stolen and subsequently published on the internet was unencrypted. California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1). Defendant notified the California Attorney General of

---

[6] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/amp/ (last visited May 19, 2022).

[7] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 19, 2022).

[8] https://www.hipaajournal.com/parker-hannifin-cyberattack-affects-almost-120000-health-plan-members/ (last visited May 19, 2022).

the Data Breach on or about May 12, 2021, evidencing that the exposed data was unencrypted.[9]

The Data Breach Was Preventable

50. Defendant could have prevented the Data Breach by properly securing and encrypting the Private Information of Plaintiffs and Class Members, by properly training its employees to recognize and prevent cybersecurity risks, and/or by implementing and following adequate retention policies to destroy the data it no longer needed. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members was exacerbated by the repeated warnings and alerts directed to U.S. companies warning that they should protect and secure sensitive data, especially in light of the substantial increase in cyberattacks specifically by the Conti ransomware group.

The Conti Ransomware Attack Was Foreseeable

51. The FBI has been warning companies, such as Defendant, about the threat posed by the Conti ransomware group, and to be on the lookout for attacks from this group, for a year. It issued a Flash Alert about Conti ransomware attacks in May 2021, and a Joint Cybersecurity Advisory on September 22, 2021, which was updated most recently on March 9, 2022 – two days before this attack took place. The Advisory was disseminated with details about what red flags indicate a business has been compromised by Conti ransomware, and how attacks can be avoided.

52. Specifically, as early as May 20, 2021, the FBI issued a Flash Alert that detailed the threat posed by the Conti group. It highlighted that "among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors

[9] https://oag.ca.gov/privacy/databreach/list (last visited May 19, 2022).

through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors."[10]

53. In the initial FBI Flash Alert, the FBI included a lengthy list of recommended mitigations that businesses should take in order to avoid or minimize the effects of a Conti attack, including:

- Regularly back up data, air gap, and password protect backup copies offline.
- Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Require administrator credentials to install software.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.

[10] FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks (May 20, 2021); https://www.ic3.gov/Media/News/2021/210521.pdf

- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training.
- Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).[11]

54. Defendant, a multibillion-dollar corporation, with sensitive government defense contracts and troves of sensitive employee information, either knew or should have known, and should have taken steps to prevent, Conti's widely publicized methods of attack.

55. The specifics of Conti's attack practices are well documented. Public reports by cybersecurity firms, such as a November 11, 2021 threat analysis report from the Cybereason Global SOC Team, walk readers step by step through Conti's methods of attack and how such attacks can be prevented.[12]

56. Moreover, on September 22, 2021, in continuing efforts to alert businesses and their employees about the growing Conti threat, the FBI and NSA sent out a warning about the Conti group over Twitter, with a call to take "immediate action." (tweet from @NSACyber last accessed May 19, 2022 below).

[11] *Id.*

[12] https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware (last visited May 19, 2022).

57. On that same day, September 22, 2021, the U.S. Cybersecurity & Infrastructure Security Agency ("CISA"), in conjunction with the FBI and NSA published a Joint Cybersecurity Advisory on Conti Ransomware.[13] These agencies reported that more than 400 Conti ransomware attacks had taken place against U.S. and international organizations.[14] According to these groups,

[13] *See*, Joint Cybersecurity Advisory: Conti Ransomware (9/22/21); https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_ WHITE.pdf (last visited July 13, 2022).

[14] *Id.*

"Conti actors frequently use a double extortion tactic: if the victim refuses to pay for data decryption, the malicious actor threatens to leak the data or sell it for profit."[15]

58. In that Joint Cybersecurity Advisory, CISA provided businesses with a lengthy listing of technical details that explained how the group was gaining initial access to business IT networks, indicators that would let businesses know they had been compromised, techniques used by Conti to compromise IT systems, and yet again, another list of recommended mitigations to reduce the risk of compromise from Conti ransomware attacks, with additional mitigations not previously included in the FBI Flash Alert.[16] The 10-page technical treatise also provided references to other helpful materials for businesses with links, and an offer for "Free Cyber Hygiene Services" offered by CISA to help organizations "assess, identify, and reduce their exposure to threats, including ransomware."[17] The increase in such attacks, and the attendant risk of future attacks, was widely known within Defendant's business community. Due to the high-profile nature of these breaches and attacks, Defendant either was or should have been on heightened notice and aware of such attacks and, therefore, should have been on notice of its duty to be proactive in guarding against being subject to such attacks and adequately performed its duty of preparing for and immediately identifying such an attack.

59. Despite the sophistication of Conti and its ransomware, it must still rely on rudimentary tactics for deploying malware on data rich systems, such as basic phishing emails.[18] Such attacks are entirely preventable through proper training of employees to recognize phishing

[15] https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware (last visited July 13, 2022).
[16] *Id*.
[17] *Id*., at p. 9.
[18] https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware (last visited May 19, 2022).

emails in combination with industry standard security measures such as required two-factor or multi-factor authentication to access email accounts and/or other computer systems.

60. Even with a successful initial infection vector through basic phishing techniques, Conti ransomware attacks may be identified and prevented by widely available software, such as the Cyberreason Defense Platform, which is known to "fully detect[] and prevent[] the Conti ransomware."[19]

61. Despite the well-known risks, Defendant inexplicably failed to properly train employees, failed to implement industry standard security measures, and maintained highly sensitive employee information in a manner it knew or should have known was vulnerable to access and exfiltration.

62. Despite the prevalence of public announcements of these data breach and data security compromises and despite numerous attempts on the part of the federal government to inform government contractor companies, like Defendant, of the threat posed by ransomware attacks in general and Conti in particular, and despite having almost a year from its attack to prepare and prevent such an attack, Defendant was negligent and did not adequately prepare for this wholly foreseeable event; thus, allowing extremely sensitive data to be accessed, viewed and stolen by the Conti ransomware group. Defendant breached its duty to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised and failed to adequately notify such persons that such a ransomware attack has taken place.

63. Unfortunately for Plaintiffs and other similarly situated individuals, their Private Information was not secured in the manner required by law that would have prevented this Conti attack.

[19] *Id.*

64. What is worse, despite Defendant's obligations under the law to promptly notify affected individuals so they can take appropriate action, Defendant failed to promptly provide such notice in the most expedient time possible and without unreasonable delay, failed to include in the Data Breach Notice Letter a sufficient description of the Data Breach, and failed to provide in the Data Breach Notice Letter the information needed by Plaintiffs and other similarly situated individuals to enable them to react appropriately to the Data Breach, including taking whatever mitigation measures are necessary.

65. As a result, this unauthorized access, disclosure, and exfiltration remains unremedied, and as detailed below the "cure" offered by Defendant to address these failures after the fact was wholly inadequate.

66. Defendant had specific obligations imposed on it by contracts and law to ensure the adequate protection of such information. For example, as federal government contractors, Defendant made representations that it would comply with numerous cybersecurity requirements applicable to the protection of data on its computer systems, including but not limited to Federal Acquisition Regulation 52.204-21 and Defense Federal Acquisition Regulation Supplement 252.204-7012, which impose physical and cybersecurity obligations on contractor systems that process government information.

Defendant's HIPAA Violations

67. In addition, to the extent that protected health information was affected by the Data Breach, as Defendant may be an entity covered by the Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security

Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards and duties for Defendant's protection of medical information maintained in electronic form.

68. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

69. "Electronic protected health information" is defined as "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

70. HIPAA's Security Rule requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance by its workforce.

71. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and also to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

72. The ransomware attack on Defendant, particularly in light of the information received almost a year before the attack, establishes that it did not comply with these Rules. This

attack resulted from a combination of inadequacies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to, the following:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

(d) Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

(e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, et seq.;

(i) Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and,

(j) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

Parker Violated Federal Trade Commission Guidelines

73. Defendant also violated the duties applicable to it under the Federal Trade Commission Act (15 U.S.C. § 45 et seq.) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC, pursuant to that Act, has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

74. As established by these laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the medical information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant also owed a duty to Plaintiffs and Class Members to provide reasonable security in compliance with industry standards and state and federal requirements, and to ensure that its computer systems, networks, and protocols adequately protected this medical information and were not exposed to infiltration. This also included a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems to ensure that the Private Information and medical information was adequately secured and protected; to create

and implement reasonable data security practices and procedures to protect the Private Information and medical information in its possession, and avoid access to its systems through processes such as phishing, including adequately training employees and others who accessed information within its systems on how to adequately protect this information and avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of its data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private Information; and to disclose in a timely and accurate manner when data breaches or ransomware attacks occurred.

75. Defendant also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems. It is apparent from the data accessed that Defendant did not do so.

76. Defendant owed these duties to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant affirmatively chose to design these systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols. These affirmative decisions resulted in Conti being able to execute the ransomware attack and exfiltrate the data in question, to the injury and detriment of Plaintiffs and Class Members. By taking affirmative acts inconsistent with these obligations that left Defendant's computer systems vulnerable to a ransomware attack, Defendant disclosed and/or permitted the disclosure of Private Information and medical information to unauthorized third parties. Defendant thus failed to preserve the confidentiality of Private Information it was duty-bound to protect.

Value of Personally Identifiable Information

77. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[20] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

78. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

79. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

---

[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 17, 2022).

[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan. 17, 2022).

[22] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 13, 2021).

evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

80. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

81. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.

82. Indeed, a robust cyber black market exists in which criminals post stolen Medical Information, PII and PHI on multiple underground internet websites, commonly referred to as the dark web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for illegal use or resale. According to a 2017 Javelin strategy and research presentation, fraudulent activities based on data stolen in data breaches that are between two and six years old had increased by nearly 400% over the previous four years.[24] Thus, an offer of credit monitoring service that is only for two years is not an adequate remedy or offer, even if it conducts dark web scanning (which is unclear here).

---

[23] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 17, 2022).

[24] *See,* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web* (2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 23, 2022).

83. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending upon completeness.[25] PII and PHI can be sold at a price ranging from approximately $20 to $300.[26]

84. In this case, all evidence indicates that Plaintiffs' and Class Members' Private Information was left unprotected, to be freely accessed on the internet by the Conti group after exfiltration. Thus, this highly valuable data was left to be pilfered by criminals or reviewed by anyone with an Internet connection – and has been accessed at least 17,000 times already.

85. Medical identity theft can also result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences since if a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[27]

86. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 to resolve per incident, and that victims often have to pay off the imposter's medical bills to resolve the breach.[28]

---

[25] *Id.*

[26] https://www.privacyaffairs.com/dark-web-price-index-2021/

[27] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, (2/7/14), https://khn.org/news/rise-of-indentity-theft/ (last visited May 3, 2022); See also, Medical Identity Theft in the New Age of Virtual Healthcare, IDX (March 15, 2021), https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last visited May 3, 2022).

[28] Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited May 3, 2022).

87. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[29]

88. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security numbers and names, is impossible to "close" and difficult, if not impossible, to change.

89. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[30]

90. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

91. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

---

[29] Ponemon Institute, Fifth Annual Study on Medical Identity Theft, (February, 2015), http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last visited May 3, 2022).

[30] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 17, 2022).

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

92. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

93. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

94. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

95. To date, Defendant has offered Plaintiffs and Class Members only two years of identity theft detection services. The offered service is wholly inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here, and is not an adequate cure of the Data Breach.

96. Specifically, Defendant did not pay the ransom or otherwise prevent the Conti ransomware group from disclosing Plaintiffs' and Class Members' Private Information on the internet. Defendant has not retrieved the Private Information taken from its systems and those systems of the Parker-Hannifin Corporation Group Health Plans. Thus, that Private Information

---

[31] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov /assets/gao-07-737.pdf (last visited Jan. 17, 2022).

remains in circulation on the internet for access, viewing, and misuse, causing damage to Plaintiffs and Class Members and breaching their confidentiality.

97. Defendant has not provided sufficient information in its Data Breach Notice Letter such that Plaintiffs and Class Members could understand and appreciate the full nature of the risk to them caused by Defendant's Data Breach, allowing them to make informed decisions about how to protect themselves and their Private Information.

98. Defendant has not provided credit monitoring and identity theft protection to Plaintiffs and Class Members for a long enough period of time, limiting the bulk of the protection services to 2 years even though this data may be used for years after that.

99. Defendant's identity theft protection offer of Experian's IdentityWorks 3B does not prevent fraudulent transactions, such as unauthorized credit card charges or exchanges of Plaintiffs' Private Information on the dark web from occurring using the Private Information disclosed by Defendant. Further, IdentityWorks 3B does not provide 3-Bureau Credit Report & FICO Scores monthly, unlike other Experian products.

100. Enrollment in IdentityWorks 3B requires Plaintiffs and Class Members to disclose Private Information to Experian, a company that had its own data breach in 2015 exposing the personal information of approximately 15 million individuals.

101. Additionally, Defendant has not taken the actions necessary and recommended by the FBI, CISA, NSA and other experts detailed above to prevent an attack by Conti or other similar group from happening again, leaving Plaintiffs and Class Members vulnerable to subsequent breaches of their Private Information held by Defendant.

102. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private

Information of Plaintiffs and Class Members.

PLAINTIFFS' EXPERIENCES

Plaintiff Christiansen

103. Plaintiff Christiansen is a former employee of Defendant and was last employed by Defendant in the late 1980's or early 1990's in Grantsburg, Wisconsin. As a condition of her employment, Plaintiff Christiansen provided her Private Information to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use her Private Information for legitimate business purposes. At no time before or after her employment did she authorize or expect Defendant to hold her Private Information for over thirty years. And she had no reasonable expectation or notice that Defendant would retain her Private Information indefinitely.

104. In maintaining Plaintiff Christiansen's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Christiansen's Private Information. Defendant assumed obligations to Plaintiff Christiansen, and she relied on Defendant to safeguard the Private Information and only utilize it for legitimate business purposes. Defendant, however, did not take proper care of Plaintiff Christiansen's Private Information, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies.

105. Plaintiff Christiansen typically takes measures to protect her Private Information and is very careful about sharing her Private Information. Had Plaintiff Christiansen known her data was still retained following her employment, Plaintiff Christiansen would have demanded that the Private Information be deleted from Parker's systems.

106. On or about May 10, 2022, Plaintiff Christiansen received notice from Defendant that her Private Information had been improperly accessed and/or obtained by unauthorized third

parties. This notice indicated that Plaintiff Christiansen's Private Information, including her Social Security number, date of birth, address, driver's license number, U.S. passport number, financial account information (bank account and routing numbers), and online account username/password was compromised as a result of the Data Breach. The letter further stated that if she is "a current or former member of Parker's Group Health Plan (or a health plan sponsored by an entity acquired by Parker)," additional Private Information, such as her enrollment information, health insurance plan member ID number, and dates of coverage may also be included.

107. As a result of the Data Breach, Plaintiff Christiansen made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing her financial accounts for any indications of actual or attempted identity theft or fraud; and researching civil attorneys in the Minnesota area. Plaintiff Christiansen has spent approximately eight (8) hours dealing with the Data Breach, valuable time Plaintiff Christiansen otherwise would have spent on other activities, including but not limited to work and/or recreation.

108. As a result of the Data Breach, Plaintiff Christiansen has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Christiansen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

109. Plaintiff Christiansen suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Christiansen; (b) violation of her privacy rights; and (c) present, imminent and

impending injury arising from the increased risk of identity theft and fraud.

110. As a result of the Data Breach, Plaintiff Christiansen also experienced actual fraud. In June 2022, Plaintiff Christiansen was notified by her credit card company, Destiny Mastercard, that her account had been compromised and a new credit card would be issued to her.

111. As a result of the Data Breach, Plaintiff Christiansen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Christiansen is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Doe

112. Plaintiff Doe, in the course of his employment with Defendant or a subsidiary thereof, was required to provide and did provide his sensitive Private Information. Plaintiff Doe was also a former enrollee of Defendant's Group Health Plan and, in connection therewith, also provided Defendant with individually identifiable information and Medical Information, as defined by Cal. Civil Code section 56.05(i).

113. In maintaining Plaintiff Doe's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Doe's Private Information. Defendant assumed obligations to Plaintiff Doe, and he relied on Defendant to safeguard the Private Information and only utilize it for legitimate business purposes. Defendant, however, did not take proper care of Plaintiff Doe's Private Information, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies.

114. Plaintiff Doe typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Had Plaintiff Doe known his data was still retained following his employment, Plaintiff Doe would have demanded that the Private Information be

deleted from Parker's systems.

115. On or about May 10, 2022, Plaintiff Doe received notice from Defendant that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Doe's Private Information, including his Social Security number, date of birth, address, driver's license number, U.S. passport number, financial account information (bank account and routing numbers), and online account username/password was compromised as a result of the Data Breach. The letter further stated that if he is "a current or former member of Parker's Group Health Plan (or a health plan sponsored by an entity acquired by Parker)," additional Private Information, such as his enrollment information, health insurance plan member ID number, and dates of coverage may also be included.

116. While Defendant has yet to provide the particulars to Plaintiffs or the Class, it is likely some amount of Plaintiff Doe's Medical Information was created, maintained, preserved, and stored onto Defendant's computer network that was accessed and disclosed during the Data Breach. Such Medical Information also likely included or contained an element of personal identifying information sufficient to allow identification of the individual, such as name, date of birth, address, and Social Security number, and additionally likely also contained medical record number, insurance provider, electronic mail address, telephone number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff Doe's identity.

117. As a result of the Data Breach, Plaintiff Doe made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: spending approximately two (2) hours researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Doe also spent approximately eight (8) hours researching the credit monitoring and identity theft protection services offered by

Defendant, creating accounts with the three credit reporting agencies so he could put a freeze on his credit in order to prevent any unauthorized use of his social security number that was disclosed by Defendant in the Data Breach, and signing up for the Experian IdentityWorks offered by Defendant. After researching and retaining counsel, Plaintiff Doe spent approximately eighteen (18) hours working with his attorneys regarding the Data Breach. Altogether, Plaintiff Doe has spent at least twenty-eight (28) hours dealing with the Data Breach to date, valuable time Plaintiff Doe otherwise would have spent on other activities. Plaintiff Doe also will continue to spend time closely monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud.

118. As a result of the Data Breach, Plaintiff Doe has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Doe is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

119. Plaintiff Doe suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Doe; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

120. Plaintiff Doe has discovered through one of the credit reporting agencies that his personal information has been exposed on the Dark Web at least twenty-six (26) times. Plaintiff Doe believes this to be a result of the Data Breach.

121. As a result of the Data Breach, Plaintiff Doe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Doe is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Harris

122. Plaintiff Harris is a former employee of Defendant and was last employed by Defendant in April 2019. As a condition of her employment, Plaintiff Harris provided her Private Information to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use her Private Information for legitimate business purposes. At no time before or after her employment did she authorize or expect Defendant to hold Private Information for longer than it had a legitimate business need. And she had no reasonable expectation or notice that Defendant would retain her Private Information indefinitely.

123. In maintaining Plaintiff Harris's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Harris's Private Information. Defendant assumed obligations to Plaintiff Harris, and she relied on Defendant to safeguard the Private Information and only utilize it for legitimate business purposes. Defendant, however, did not take proper care of Plaintiff Harris's Private Information, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies.

124. Plaintiff Harris typically takes measures to protect her Private Information and is very careful about sharing her Private Information. Had Plaintiff Harris known her data was still retained following her employment, Plaintiff Harris would have demanded that the Private Information be deleted from Parker's systems.

125. On or about May 24, 2022, Plaintiff Harris received notice from Defendant that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice, dated May 10, 2022, indicated that Plaintiff Harris's Private Information, including her Social Security number, date of birth, address, driver's license number, U.S. passport number, financial account information (bank account and routing numbers), online account username/password. The letter further stated that if she is "a current or former member of Parker's Group Health Plan (or a health plan sponsored by an entity acquired by Parker)," additional Private Information, such as his enrollment information, health insurance plan member ID number, and dates of coverage may also be included.

126. As a result of the Data Breach, Plaintiff Harris made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Harris has spent at least fifteen (15) hours dealing with the Data Breach, valuable time Plaintiff Harris otherwise would have spent on other activities. Plaintiff Harris spent approximately eight (8) hours reviewing the data breach notification letter, reviewing the included credit monitoring information, researching the data breach online, reviewing Facebook posts about the data breach, signing up for the credit monitoring offer, and reviewing all her financial accounts for any fraudulent activity. Since receiving the Data Breach notification letter, Plaintiff Harris has also spent approximately one (1) hour per week checking on all of her financial accounts.

127. Plaintiff Harris has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information

for purposes of identity theft and fraud. Plaintiff Harris is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

128. Plaintiff Harris suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Harris; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

129. As a result of the Data Breach, Plaintiff Harris anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Harris is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff McCormick

130. Plaintiff McCormick worked with Defendant from 2010 to 2011 in the Veriflo division in Richmond, California.

131. As a condition of his employment, Plaintiff McCormick provided his Private Information to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use his Private Information for legitimate business purposes. At no time before or after his employment did he authorize or expect Defendant to hold Private Information for longer than it had a legitimate business need. And he had no reasonable expectation or notice that Defendant would retain his Private Information indefinitely.

132. Plaintiff McCormick typically takes measures to protect his Private Information and is very careful about sharing his Private Information. He monitors his accounts and credit

scores, and has sustained emotional distress as a result of worrying about his Private Information being exfiltrated. Further Plaintiff McCormick has alerted Experian about his Private Information being compromised in the Data Breach and has also instituted a credit freeze. This is time that was and will be lost and unproductive and taken from other activities and duties.

133. Plaintiff McCormick received notice from Defendant that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice, dated May 10, 2022, indicated that Plaintiff McCormick's Private Information, including his Social Security number, date of birth, address, driver's license number, U.S. passport number, financial account information (bank account and routing numbers), and online account username/password. The letter further stated that if he is "a current or former member of Parker's Group Health Plan (or a health plan sponsored by an entity acquired by Parker)," additional Private Information, such as his enrollment information, health insurance plan member ID number, and dates of coverage may also be included.

134. Plaintiff McCormick suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and had anxiety, emotional distress, and increased concerns for the loss of his privacy and will continue to for years to come.

135. Plaintiff McCormick has already experienced fraudulent activity on his bank accounts after the Data Breach. Notably, an unauthorized person opened two fraudulent bank accounts at Trust Bank in his name. Plaintiff McCormick did not authorize or even know about the opening of either of these bank accounts. Plaintiff McCormick closed his checking account to try to protect himself from further fraud resulting from the Data Breach. For example, he had to close a checking and savings account he had for twenty years at the Bank of the West because it was compromised after the Data Breach.

136. Additionally, even after placing alerts on his bank and credit accounts, four accounts (two checking and two savings) were opened under Plaintiff McCormick's name at Truist Bank without his authorization. He received notification of these fraudulent accounts from Truist Bank on June 2, 2022 noting that he was a victim of identity theft. Furthermore, after the Data Breach, a checking account was opened at CapitalOne in Plaintiff McCormick's name without his authorization, and an unauthorized Bank of America savings account was opened in Plaintiff McCormick's name after the Data Breach.

137. As a result of the Data Breach, Plaintiff McCormick has resorted to paying his bills via money order because of all the fraudulent activities on his bank accounts. He is charged a fee for each money order transaction. These fees are out-of-pocket losses Plaintiff McCormick has suffered as a result of the Data Breach.

138. As a result of the Data Breach and the unauthorized exfiltration and publication of his unencrypted Private Information by malicious cybercriminals, Plaintiff McCormick is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

139. To date, Defendant has done very little to adequately protect Plaintiff McCormick and Class Members, or to compensate them for their injuries sustained in this Data Breach. It offered identity monitoring services, but only for two years, which is wholly inadequate for a data breach including Plaintiff McCormick's and Class Members' Social Security numbers.

Plaintiff Migliaccio

140. Plaintiff Joan Migliaccio received the Notice Letter dated May 10, 2022.

141. Plaintiff Migliaccio's husband was employed at Parker in the early to mid-1980s, and her information was recorded and stored on Parker's systems when her husband signed up for

Parker's employee benefits.

142. In acquiring and maintaining Plaintiff Migliaccio's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Migliaccio's Private Information. Plaintiff Migliaccio was the intended beneficiary of the employee benefits of her husband, and she received such benefits as an intended direct beneficiary. Defendant, however, did not take proper care of Plaintiff Migliaccio's Private Information, leading to its exposure as a direct result of Defendant's inadequate security measures and data retention policies.

143. Plaintiff Migliaccio typically takes measures to protect her Private Information and is very careful about sharing her Private Information. Had Plaintiff Migliaccio known her data was still retained by Defendant, Plaintiff Migliaccio would have demanded that the Private Information be deleted from Parker's systems.

144. Given the highly sensitive nature of the information stolen and disseminated in the Data Breach, Plaintiff Migliaccio is, and will continue to be into the future, at an imminent risk of identity theft and fraud. Plaintiff Migliaccio is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

145. In response to the Data Breach and the Notice Letter, Plaintiff Migliaccio immediately began taking steps to protect herself and her identity. She made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Migliaccio has spent several hours dealing with the Data Breach, valuable time Plaintiff Migliaccio otherwise would have spent on other activities, including but not limited to work and/or recreation.

146. As a direct result of the Data Breach, Plaintiff Migliaccio has suffered actual injury including, but not limited to: (a) violation of her privacy rights; (b) damage to and diminution in the value of her Private Information; (c) loss of present and future time mitigating the imminent risk of identity theft; and (d) she will incur future costs for identity theft protection.

Plaintiff Mulanax

147. Plaintiff Mulanax retired from Defendant in August 2012. As a condition of her employment, Plaintiff Mulanax provided her Private Information to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use her Private Information for legitimate business purposes. At no time before or after her employment did she authorize or expect Defendant to hold her Private Information for over a decade. And she had no reasonable expectation or notice that Defendant would retain her Private Information indefinitely.

148. In maintaining Plaintiff Mulanax's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Mulanax's Private Information. Defendant assumed obligations to Plaintiff Mulanax, and she relied on Defendant to safeguard the Private Information and only utilize it for legitimate business purposes. Defendant, however, did not take proper care of Plaintiff Mulanax's Private Information, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies.

149. Plaintiff Mulanax typically takes measures to protect her Private Information and is very careful about sharing her Private Information. Had Plaintiff Mulanax known her data was still retained following her employment, Plaintiff Mulanax would have demanded that the Private Information be deleted from Parker's systems.

150. On or about May 18, 2022, Plaintiff Mulanax returned from vacation to find the

Notice Letter from Defendant dated May 10, 2022 informing her that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Mulanax's Private Information, including her Social Security number, date of birth, address, driver's license number, U.S. passport number, financial account information (bank account and routing numbers), and online account username/password was compromised as a result of the Data Breach.

151. As a result of the Data Breach, Plaintiff Mulanax made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Mulanax has spent a total of approximately sixteen (16) hours dealing with the Data Breach, valuable time Plaintiff Mulanax otherwise would have spent on other activities. Plaintiff Mulanax spent approximately eight (8) hours reviewing the data breach notification letter, reviewing the Experian IdentityWorks credit monitoring terms, reviewing what employment records of hers that Defendant may have, researching common effects from data breaches, and researching the bank account that she used for direct deposit while working for Defendant. Plaintiff Mulanax spent another approximately eight (8) hours researching new banks, how to open new bank accounts, and opening a new bank account because she was fearful that her current bank account was compromised in the Data Breach. Plaintiff Mulanax spent time cancelling her incoming automatic pension and social security payments to her current bank account. Plaintiff Mulanax will also have to spend time in the future updating approximately thirty-five (35) accounts that will have to be switched to her new bank account information, as well as setting up new direct deposit for her pension and social security payments.

152. As a result of the Data Breach, Plaintiff Mulanax has suffered anxiety as a result of the release of her Private Information , which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Mulanax is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

153. Plaintiff Mulanax suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Mulanax; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

Plaintiff Rosal

149. Plaintiff Rosal's employment with Defendant ended in 2015. As a condition of his employment, Plaintiff Rosal provided his Private Information to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use his Private Information for legitimate business purposes. At no time before or after his employment did he authorize or expect Defendant to hold his Private Information indefinitely. And he had no reasonable expectation or notice that Defendant would retain his Private Information indefinitely.

150. In maintaining Plaintiff Rosal's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Rosal's Private Information. Defendant assumed obligations to Plaintiff Rosal, and he relied on Defendant to safeguard the Private Information and only utilize it for legitimate business purposes. Defendant, however, did not take proper care of

Plaintiff Rosal's Private Information, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies.

151. Plaintiff Rosal typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Had Plaintiff Rosal known his data was still retained following his employment, Plaintiff Rosal would have demanded that the Private Information be deleted from Parker's systems.

152. Shortly after May 10, 2022, Plaintiff Rosal received notice from Defendant that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Rosal's Private Information, including his Social Security number, date of birth, address, driver's license number, U.S. passport number, financial account information (bank account and routing numbers), and online account username/password was compromised as a result of the Data Breach.

153. As a result of the Data Breach, Plaintiff Rosal made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Rosal has also had to freeze his credit in order to prevent any unauthorized use of his social security number that was disclosed by Defendant in the Data Breach. Plaintiff Rosal also had to spend time addressing unauthorized charges on his checking account debit card and his checking account that occurred sometime in May 2022. Due to the unauthorized charges, Plaintiff Rosal had to close the debit card and get a new debit card. To date, Plaintiff Rosal has spent at least thirty (30) hours dealing with the Data Breach, valuable time Plaintiff Rosal otherwise would have spent on other activities, including but not limited to work and/or recreation.

154. As a result of the Data Breach, Plaintiff Rosal has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Rosal is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

155. Plaintiff Rosal suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Rosal; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

156. As a result of the Data Breach, Plaintiff Rosal has also experienced actual fraud in the form of unauthorized charges on his checking account debit card and his checking account.

157. As a result of the Data Breach, Plaintiff Rosal anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rosal is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Rowe

158. Plaintiff Rowe's employment with Defendant ended in 1999. As a condition of his employment, Plaintiff Rowe provided his Private Information to Defendant with the reasonable expectation that Defendant would maintain such information in a secure manner, would implement reasonable data retention policies, and would only use his Private Information for legitimate business purposes. At no time before or after his employment did he authorize or expect Defendant

to hold his Private Information indefinitely. And he had no reasonable expectation or notice that Defendant would retain his Private Information indefinitely.

159. In maintaining Plaintiff Rowe's Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Rowe's Private Information. Defendant assumed obligations to Plaintiff Rowe, and he relied on Defendant to safeguard the Private Information and only utilize it for legitimate business purposes. Defendant, however, did not take proper care of Plaintiff Rowe's Private Information, leading to its exposure as a direct result of Defendant's inadequate security measures and negligent data retention policies.

160. Plaintiff Rowe typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Had Plaintiff Rowe known his data was still retained following his employment, Plaintiff Rowe would have demanded that the Private Information be deleted from Parker's systems.

161. Shortly after May 10, 2022, Plaintiff Rowe received notice from Defendant that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Rowe's Private Information, including his Social Security number, date of birth, address, driver's license number, U.S. passport number, financial account information (bank account and routing numbers), and online account username/password was compromised as a result of the Data Breach. The letter further stated that if she is "a current or former member of Parker's Group Health Plan (or a health plan sponsored by an entity acquired by Parker)," additional Private Information, such as her enrollment information, health insurance plan member ID number, and dates of coverage may also be included.

162. As a result of the Data Breach, Plaintiff Rowe made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing

credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Rowe has also spent time, averaging thirty (30) minutes a day, determining whether potentially fraudulent emails, texts, and calls are legitimate. To date, Plaintiff Rowe has spent at least twenty (20) hours dealing with the Data Breach, valuable time Plaintiff Rowe otherwise would have spent on other activities.

163. As a result of the Data Breach, Plaintiff Rowe has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Rowe is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

164. Plaintiff Rowe suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Rowe; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

165. Plaintiff Rowe has also experienced a substantial increase in suspicious and "spam" telephone calls and emails since the Data Breach. Plaintiff Rowe believes these suspicious telephone calls and emails to be a result of the Data Breach.

166. As a result of the Data Breach, Plaintiff Rowe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rowe is at a present risk and will continue to be

at increased risk of identity theft and fraud for years to come.

Plaintiff Yancey

167. Plaintiff Yancey received the Notice Letter from Defendant dated May 10, 2022.

168. Plaintiff Yancey was a dependent of a former employee of Defendant, and he was unaware that Defendant had possession of his Private Information. At no time did he authorize Defendant to hold his Private Information for non-legitimate business purposes.

169. Plaintiff Yancey typically takes measures to protect his Private Information and is very careful about sharing her Private Information. Had Plaintiff Yancey been aware that Defendant held his information, he would have demanded that his Private Information be deleted from Defendant's systems.

170. Given the highly sensitive nature of the information stolen and disseminated in the Data Breach, Plaintiff Yancey is, and will continue to be into the future, at an imminent risk of identity theft and fraud. Plaintiff Yancey is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

171. As a result of the Data Breach, Plaintiff Yancey made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Yancey has spent between 20 and 30 hours dealing with the Data Breach, valuable time Plaintiff Yancey otherwise would have spent on other activities, including but not limited to work and/or recreation.

172. Plaintiff Yancey has also experienced a substantial increase in suspicious and "spam" telephone calls and emails since the Data Breach. Plaintiff Yancey believes these

suspicious telephone calls and emails to be a result of the Data Breach.

173. Plaintiff Yancey suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Yancey; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

CLASS ACTION ALLEGATIONS

174. Plaintiffs bring this nationwide class action on behalf of themselves and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

175. The Nationwide Class is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

176. The California Subclass is defined as follows:

> **All California residents that Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

177. The New York Subclass is defined as follows:

> **All New York residents that Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

178. Excluded from the Class and Subclasses are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

179. Plaintiffs reserve the right to amend or modify the Class definitions and/or create additional subclasses as this case progresses.

180. Numerosity. The members of the Class and Subclasses are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time the Classes consists of more than 125,000 current and former employees of Defendant and acquired subsidiaries whose sensitive data was compromised in Data Breach.

181. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

m. Whether Defendant violated the consumer protection statute invoked below;

n. Whether Defendant breach implied or express contracts with Plaintiffs and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiffs and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

q. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

182. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

183. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' counsel are competent and experienced in litigating class actions.

184. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the

same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

185. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

186. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
Negligence
(on behalf of Plaintiffs and the Nationwide Class)

187. Plaintiffs re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein.

188. As a condition of applying for jobs and/or maintaining employment with Defendant or enrolling in its health plans, Plaintiffs and the Nationwide Class were obligated to provide Defendant with their Private Information.

189. Plaintiffs and the Nationwide Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would exercise reasonable care in the protection of their Private Information.

190. Defendant had a duty to take reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. This duty is inherent in the nature of the exchange of highly sensitive personal information.

191. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the Private Information were wrongfully disclosed.

192. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, using, and retaining of the Private Information of Plaintiffs and the Nationwide Class, without adequate data security, involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class.

193. Defendant had a duty to exercise reasonable care in safeguarding, securing, retaining, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, design, configuring, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

194. Defendant also had a duty to exercise appropriate clearinghouse practices to remove job applicants' Private Information that it was no longer required to retain pursuant to regulations.

195. Defendant had a duty to properly train employees to recognize phishing attempts and other common data security risks.

196. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Nationwide Class.

197. Defendant's duty to use reasonable security measures arose, and was assumed, as a result of the relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That relationship arose, and was assumed, because Plaintiffs and the Nationwide Class entrusted Defendant with their confidential Private Information and relied upon Defendant to implement adequate data security and reasonable data retention policies.

198. Defendant was subject to an independent duty untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

199. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, and other public data breaches in the news and common knowledge.

200. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that Private Information, the necessity for encrypting Private Information, and the harm that can arise from retaining Private Information following the expiration of any legitimate business purpose.

201. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to encrypt the data stored on its system, failure to implement other reasonable industry standard measures to safeguard Private Information, and its failure to implement retention policies that deletes unnecessary Private Information from its systems.

202. Plaintiffs and the Nationwide Class had no ability to protect their Private Information that was in, and remains in, Defendant's possession.

203. Defendant had a duty to warn former employees that their Private Information would be retained many years past the point of employment, and in some cases, indefinitely.

204. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

205. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

206. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Nationwide Class.

207. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the

Nationwide Class during the time the Private Information was within Defendant's possession or control.

208. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

209. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of job applicants' Private Information.

210. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove job applicants' Private Information that it was no longer required to retain pursuant to regulations.

211. Defendant breached its duty to adequately train employees to recognize and avoid phishing attempts and other basic cybersecurity risks.

212. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

213. Defendant breached its duty to safeguard Plaintiffs' and Nationwide Class Members' Private Information by failing to retain such information in an encrypted form.

214. Defendant breached its duty to safeguard Plaintiffs' and Nationwide Class Members' Private Information by retaining the information for many years including for several decades regardless of whether the current or former employee remained employed with Defendant.

215. Defendant breached its duty to safeguard Plaintiffs' and Nationwide Class Members' Private Information by failing to warn or advise former employees that their Private

Information would be retained many years past the point of employment, and in some cases, indefinitely.

216. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Private Information of Plaintiffs and the Nationwide Class would not have been compromised.

217. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The Private Information of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

218. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and the Nationwide Class Members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

219. As Defendant instructed, advised, and warned in its Notice Letters, Plaintiffs and the Nationwide Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Nationwide Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included, and will include into the future, protective steps: e.g., reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

220. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and Nationwide Class Members have suffered actual and concrete injuries and will suffer addition injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the Notice Letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring for the Nationwide Class; (g) loss of time incurred due to actual identity theft; (h) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (i) and diminution of value of their Private Information.

221. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession. Plaintiffs and Nationwide Class Members are, therefore, also seeking injunctive relief for the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the Private Information.

222. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Negligence *per se*
(on behalf of Plaintiffs and the Nationwide Class)

223. Plaintiffs re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein.

224. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One*, 488 F. Supp. 3d at 407.

225. Plaintiffs' and Nationwide Class members' Private Information was and is nonpublic personal information and customer information.

226. Plaintiffs and Nationwide Class members are in the group of persons the FTC Act were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendant's violations of the FTC Act were the types of harm they are designed to prevent.

227. As a direct and proximate result of Defendant's numerous negligent acts and omissions, Plaintiffs and the Nationwide Class Members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

228. As a direct and proximate result of the conduct of Defendant that violated the FTC Act, Plaintiffs and Nationwide Class members have suffered and will continue to suffer the foreseeable economic and non-economic harms as described herein.

229. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Breach of Implied Contract
(on behalf of Plaintiffs and the Nationwide Class)

230. Plaintiffs re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein.

231. Defendant required Plaintiff and the Nationwide Class to provide their Private Information as a condition of applying for and/or maintaining employment. In so doing, Plaintiffs and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

232. Defendant further entered into an implied contract with Plaintiffs and the Nationwide Class to honor the representations discussed *infra* in its Privacy Policy.

233. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

234. Defendant breached the implied contracts it made with Plaintiffs and the Nationwide Class by (i) failing to implement reasonable technical, administrative, and physical security measures to protect the Private Information from unauthorized access or disclosure (such as encryption of Social Security numbers) despite such measures being readily available, (ii)

failing to limit access to the Private Information to Defendant's employees who needed such information to perform a specific job, (iii) failing to store the Private Information only on servers kept in a secure, restricted access area, (iv) retaining Private Information longer than necessary, and (v) otherwise failing to safeguard the Private Information.

235. As a direct and proximate result of Defendant's breach of its implied contract, Plaintiffs and the Nationwide Class Members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

236. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Nationwide Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic damages in the following forms: (a) financial costs incurred mitigating the imminent risk of identity theft; (b) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the Notice Letter; (d) financial costs incurred due to actual identity theft; (e) the cost of future identity theft monitoring for the Class; (f) loss of time incurred due to actual identity theft; (g) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls, and (h) diminution of value of their Private Information.

237. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
Unjust Enrichment
(on behalf of Plaintiffs and the Nationwide Class)

238. Plaintiffs re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein.

239. This claim is brought in the alternative to Plaintiffs' claims for breach of implied contract.

240. Defendant benefited from receiving Plaintiffs' and Nationwide Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

241. Defendant also understood and appreciated that Plaintiffs' and Nationwide Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

242. Plaintiffs and Nationwide Class Members conferred a monetary benefit upon Defendant in the form of providing an ability to find people to employ, and in connection thereto, by providing their Private Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their Private Information. In exchange, Plaintiffs and Nationwide Class Members should have received adequate protection and data security for such Private Information held by Defendant.

243. Defendant knew Plaintiffs and Nationwide Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Nationwide Class Members for business purposes.

244. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Nationwide Class Members.

245. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Nationwide Class members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

246. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Nationwide Class Members.

247. Defendant's enrichment at the expense of Plaintiffs and Nationwide Class Members is and was unjust.

248. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and Nationwide Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT V
Declaratory Relief
(on behalf of Plaintiffs and the Nationwide Class)

249. Plaintiffs re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein.

250. A present and actual controversy exists between the parties. Defendant has failed to acknowledge the wrongful nature of its actions, has not sent affected persons comprehensive data breach notices regarding the Conti ransomware attack and Data Breach at issue herein, nor publicly issued comprehensive corrective notices. Based on its inadequate disclosures to date, there is also no reason to believe that Defendant has taken adequate measures to correct or enact adequate privacy policies and revised its IT and computer systems to protect and preserve

Plaintiffs' and the Nationwide Class Members' Personal Information and Medical Information in Defendant's possession.

251. Now that Defendant's insufficient information security is known to hackers, the Personal Information and Medical Information in Defendant's possession is even more vulnerable to cyberattack.

252. Plaintiffs and Nationwide Class Members have no other adequate remedy of law in that absent declaratory relief from the Court, Defendant is likely to not fully remedy the underlying wrong.

253. As described above, Defendant's actions have caused harm to Plaintiffs and Nationwide Class Members. Further, Plaintiffs and the Nationwide Class Members are at risk of additional or further harm due to the exposure of their Medical Information and Personal Information, and Defendant's failure to fully address the security failings that lead to such exposure and provide notice thereof.

254. Plaintiffs and the Nationwide Class seek an order of this Court for declaratory, equitable and/or injunctive relief in the form of an order finding Defendant has failed and continues to fail to adequately protect Plaintiffs' and the Nationwide Class Members' Personal Information and Medical Information from release to unknown and unauthorized third parties, requiring Defendant to correct or enact adequate privacy policies and security measures to protect and preserve Plaintiffs' and the Nationwide Class Members' Personal Information and Medical Information in its possession, and requiring Defendant to publicly issue comprehensive corrective notices to Plaintiffs, Nationwide Class Members and the public.

COUNT VI
Violations of the California Consumer Privacy Act
Cal. Civ. Code § 1798.100 *et seq*.
(on behalf of Plaintiff Doe and the California Subclass)

255. Plaintiff John Doe ("Plaintiff" for the purposes of this Count) re-alleges and incorporates by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein. This Count is brought on behalf of the California Subclass (the "Class" for the purposes of this Count).

256. The CCPA was enacted to protect consumers' sensitive information from collection and use by businesses without appropriate notice and consent.

257. Through the above-detailed conduct, Defendant violated the CCPA by subjecting the nonencrypted and nonredacted Personal Information of Plaintiff and Class Members to unauthorized access, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

258. Under the Section 1798.150(a)(1) of the CCPA, "Personal information" means an individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social Security number, (ii) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual, (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, (iv) medical information, (v) health insurance information, (vi) unique biometric data generated from measurements or technical analysis of human body

characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes, (vii) genetic data.

259. The Private Information at issue in this action falls within the types of information actionable under Cal. Civ. Code § 1798.150(a)(1), since, as described in Defendant's notification posted on its website entitled "Notice of Data Security Incident," the identified Private Information at risk to Plaintiff and Class Members due to this Data Breach is as follows:

> individuals' names in combination with one or more of the following: Social Security numbers, dates of birth, addresses, driver's license numbers, U.S. passport numbers, financial account information (bank account and routing numbers), online account usernames / passwords, enrollment information, including health insurance plan member ID numbers, and dates of coverage. For a very small number of these individuals, the files also included dates of coverage, dates of service, provider names, claims information, and medical and clinical treatment information.

260. With the exception of information regarding Plaintiff or Class Members' medical and clinical treatment information, Defendant maintained the Private Information identified above in the context of Plaintiff's employment with Defendant or an entity acquired by Defendant, separately and unrelated to any Plaintiff or Class Member's medical history, mental or physical condition, or treatment.

261. In accordance with Cal. Civ. Code § 1798.150(b), on or about June 1, 2022, Plaintiff's counsel sent a Notice of Violation to Defendant on behalf of Plaintiff and all other similarly situated California residents.

262. Defendant did timely respond to and accept Plaintiff John Doe's claim for damages, on behalf of both himself and all others similarly situated who can assert such claims. As detailed above, Defendant's offer of a cure was inadequate and did not comply with the requirements of the CCPA.

263. During the pendency of the 30-day waiting period provided for in Cal. Civ. Code § 1798.150(b), Plaintiff John Doe solely sought injunctive relief for Defendant's violation of the CCPA, in the form of an order enjoining Defendant from continuing to violate the CCPA through its failure to fulfill the duties set forth in 1798.150(a). As Defendant failed to cure the noticed violations and failed to provide Plaintiff John Doe with an express written statement within 30 days of Plaintiff's Notice of Violation that the violations have been cured and that no further violations shall occur, Plaintiff John Doe now seeks actual and punitive damages, statutory damages of between $100 and $750 per Class Member, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.

COUNT VII
Violations of the Confidentiality of Medical Information Act
Cal. Civ. Code § 56 *et seq*.
(on behalf of Plaintiffs Doe and McCormick and the California Subclass)

264. Plaintiffs John Doe and Daniel McCormick ("Plaintiffs" for the purposes of this Count) re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein. This Count is brought on behalf of the California Subclass (the "Class" for the purpose of this Count).

265. Defendant is subject to the requirements of the CMIA as an employer under Cal. Civ. Code Section 56.20(a) and as a corporation that receives Medical Information regarding a patient under California Civil Code Section 56.10(e), which as noted above it admits to having received. Defendant is not a "provider of health care" under the CMIA as defined in Cal. Civ. Code § 56.05(m) in that it is not "a person licensed or certified pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code; a person licensed pursuant to the Osteopathic Initiative Act or the Chiropractic Initiative Act; a person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code; or a clinic, health dispensary,

or health facility licensed pursuant to Division 2 (commencing with Section 1200) of the Health and Safety Code." Cal. Civ. Code § 56.05(m).

266. On May 13, 2022, the U.S. Department of Health and Human Services Office for Civil Rights identified "Parker-Hannifin Corporation Group Health Plans" as the Covered Entity responsible for the Data Breach at issue in the action.

267. According to HHS, a group health plan is considered to be a separate legal entity from the employer or other parties that sponsor a group health plan. Defendant is self-insured in the United States for health care and thus receives Medical Information from a subset of the Class in that context, even though to date Defendant has not identified who falls within the category of persons for whom Defendant held such information and whose information was exfiltrated as part of the Data Breach.

268. Defendant must not disclose or permit the disclosure of Medical Information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining authorization, subject to certain exceptions found in Civil Code Section 56.10(b) & (c) that do not apply here. Cal. Civ. Code §§ 56.10(a) & (e). Further, to the extent that Defendant was an employer of Plaintiffs and Class Members, it is prohibited from using disclosing, or knowingly permitting its employees or agents to use or disclose Medical Information that Defendant possesses pertaining to its employees without the patient having first signed an authorization, except under certain exceptions not relevant to this action. Additionally, to the extent the Defendant was an employer to Plaintiffs and Class Members, it was also required to establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of Medical Information it has received, including, but not limited to instruction regarding confidentiality to employees and agents handling files containing Medical Information,

and security systems restricting access to files containing Medical Information. By its affirmative acts and inactions set forth above, Defendant disclosed or permitted the use and/or disclosure of Medical Information to unauthorized third parties in violation of this Section, as well as failed to establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of the Medical Information it had received.

269. Defendant is required under the CMIA to ensure that it maintains, preserves, and stores Medical Information in a manner that preserves the confidentiality of the information contained therein. Cal. Civ. Code § 56.101(a) & 56.36(b).

270. Defendant is required to create, maintain, preserve, store, abandon, destroy or dispose of Medical Information in a non-negligent manner. Cal. Civ. Code § 56.101(a).

271. Plaintiffs and members of the Class are "Patients" as defined by Cal. Civ. Code section 56.05(j).

272. Certain information at issue in this action is "Medical Information" as that term is defined by section 56.05(i) of the CMIA, including, under certain circumstances, dates of medical services, provider names, claims information and medical and clinical treatment information either that, alone or in combination with other publicly available information, reveals patient identities.

273. As described above, the actions or inactions of Defendant failed to preserve the confidentiality of Medical Information, including but not limited to Plaintiffs' and Class Members' Medical Information.

274. The Medical Information that was the subject of the Conti ransomware attack and resulting Data Breach detailed above was accessed, removed, exfiltrated and actually viewed by the Conti ransomware group and its members, and other unauthorized parties during and following the ransomware attack.

275. Since the Conti ransomware group published the entirety of the almost 420 gigabytes of data it exfiltrated onto the web to be downloaded freely, the data at issue herein was viewed and the confidentiality and integrity of that data was breached, lost, not preserved, and not protected by Defendant.

276. In violation of the CMIA, Defendant disclosed or permitted the disclosure of Medical Information regarding Plaintiffs and Class Members without authorization to a third party. This disclosure did not qualify for any of the exemptions set forth in Cal. Civ. Code §§ 56.10(b) or (c), which provide limited bases for allowing unauthorized disclosures. This disclosure of Medical Information to unauthorized individuals resulted from the affirmative actions and inactions of Defendant and its employees, which allowed hackers from the Conti ransomware group to access, view and obtain the Medical Information of tens of thousands of Defendant's or its subsidiary's employees or their dependents.

277. In violation of the CMIA, Defendant, as a recipient of Medical Information pursuant to an authorization under Chapter 2 of the CMIA or pursuant to the provisions of Cal. Civ. Code § 56.10(c), further disclosed that Medical Information without a new authorization that met the requirements of Cal. Civ. Code § 56.11, and without otherwise being required or permitted by law to do so.

278. In violation of the CMIA, Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiffs and Class Members in a manner that did not preserve the confidentiality of the information contained therein.

279. In violation of the CMIA, Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiffs and Class Members.

280. In violation of the CMIA, Defendant negligently released confidential information or records concerning Plaintiffs and Class Members.

281. In violation of the CMIA, Defendant failed to give prompt, timely and fulsome notice of the Conti ransomware attack and resulting Data Breach.

282. As a direct and proximate result of Defendant's wrongful actions, inactions, omissions, and want of ordinary care that directly and proximately caused the release of Medical Information of thousands of individuals, such personal Medical Information was viewed by, released to, and disclosed to third parties without appropriate written authorization.

283. Plaintiffs and members of the California Subclass are therefore entitled to injunctive relief, actual damages, statutory damages of $1,000 per Subclass Member, punitive damages of $3,000 per Subclass Member, and reasonable attorneys' fees of $1,000 per Subclass Member and costs.

COUNT VIII
Invasion of Privacy
California Constitution, Article I, Section 1
(on behalf of Plaintiffs Doe and McCormick and the California Subclass)

284. Plaintiffs Doe and McCormick ("Plaintiffs" for the purposes of this Count) re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein. This Count is brought on behalf of the California Subclass (the "Class" for the purposes of this Count).

285. The California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I., § 1.

286. Plaintiffs and Class members had a legitimate expectation of privacy in their Personal Information and Medical Information, and were entitled to the protection of this information against disclosure to unauthorized third parties.

287. Defendant owed a duty to Plaintiffs and Class Members to keep their Personal Information and Medical Information confidential.

288. Defendant failed to protect and released to unauthorized third parties the non-redacted and non-encrypted Personal Information and Medical Information of Plaintiffs and Class Members.

289. Defendant allowed unauthorized and unknown third parties access to and examination of the Personal Information and Medical Information of Plaintiffs and Class Members by way of Defendant's affirmative actions and negligent failures to protect this information.

290. The unauthorized release to, custody of, and examination by unauthorized third parties of the Personal Information and Medical Information of Plaintiffs and Class Members is highly offensive to a reasonable person.

291. The intrusion at issue was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Personal Information and Medical Information to Defendant as part of Plaintiffs' and Class Members' relationships with Defendant, but privately and with the intention that the Personal Information and Medical Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

292. The Conti ransomware attack that resulted from the actions and inactions of Defendant constitutes an intentional interference with the Plaintiffs' and Class Members' interest

in solitude or seclusion, either as to their persons or as to their private affairs or concerns and those of their families, of a kind that would be highly offensive to a reasonable person.

293. Defendant acted with a knowing or negligent state of mind when it permitted the attack described herein to occur, because it either knew or reasonably should have known that its information security practices were inadequate and insufficient to protect again such attacks.

294. Defendant either knew or reasonably should have known that its inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

295. As a proximate result of the above acts and omissions of Defendant, the Personal Information and Medical Information, of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer injuries and damages in an amount according to proof.

296. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and the Class, entitling them to seek injunctive relief.

297. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and/or the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiffs in relation to their stake in the matter. Because this case is brought for the purposes of enforcing important rights affecting the public interest, Plaintiffs also seek the recovery of attorneys' fees and costs in prosecuting this action against Defendant under California Code of Civil Procedure section 1021.5 and other applicable law.

COUNT IX
Violations of the Unfair Competition Law
Cal. Bus. & Prof. Code § 17200 *et seq*.
(on behalf of Plaintiffs Doe and McCormick and the California Subclass)

298. Plaintiffs Doe and McCormick ("Plaintiffs" for the purposes of this Count) re-allege and incorporate by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein. This Count is brought on behalf of the California Subclass (the "Class" for the purposes of this Count).

299. The acts, misrepresentations, omissions, practices, and non-disclosures of Defendant as alleged herein constituted unlawful and unfair business acts and practices within the meaning of California Business & Professions Code sections 17200, *et seq.*

300. Defendant engaged in "unlawful" business acts and practices in violation of the California statutes set forth above, including Civil Code sections 56.10(a), 56.10(e), 56.20, 56.101, 1798.100 et seq., 1798.21, 1798.29, 1798.100 et seq., and Article I, § 1 of the California Constitution. Defendant's acts also violated federal statutes and regulations, including the Federal Trade Commission Act (15 U.S.C. § 45 et seq.). Plaintiffs reserve the right to allege other violations of law committed by Defendant that constitute unlawful business acts or practices within the meaning of California Business & Professions Code sections 17200, *et seq.*

301. Defendant has also engaged in "unfair" business acts or practices. There are several tests that determine whether a practice that impacts consumers as compared to competitors is "unfair," examining the practice's impact on the public balanced against the reasons, justifications and motives of Defendant. Defendant's conduct would qualify as "unfair" under any of these standards:

a. does the practice offend an established public policy, which here are whether the practices at issue offend the policies of protecting consumers' Personal

Information and Medical Information by engaging in illegal practices, as reflected in California law and policy set forth above;

b. balancing the utility of Defendant's conduct against the gravity of the harm created by that conduct, including whether Defendant's practices caused substantial injury to consumers with little to no countervailing legitimate benefit that could not reasonably have been avoided by the consumers themselves, and causes substantial injury to them; or

c. is the practice immoral, unethical, oppressive, unscrupulous, unconscionable or substantially injurious to consumers.

302. The harm caused by Defendant's failure to maintain adequate information security procedures and practices, including but not limited to failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions, failing to properly and adequately educate and train employees, failing to put into place reasonable or adequately protected computer systems and security practices to safeguard employees' Personal Information and Medical Information, including access restrictions, multi-factor authentication and encryption, failing to have adequate privacy policies and procedures in place that did not preserve the confidentiality of the Personal Information and Medical Information of Plaintiffs and the Class Members in its possession, failing to timely and accurately disclose the ransomware attack and resulting data breach to Plaintiffs and Class Members, and failing to protect and preserve confidentiality of Personal Information and Medical Information of Plaintiffs and Class Members against disclosure and/or release, outweighs the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical, and offensive, and causes substantial injury to Plaintiffs and Class Members.

303. Defendant either knew or should have known that Defendant's data security and protection practices were inadequate to safeguard the Personal Information and Medical Information of Plaintiffs and Class Members, deter hackers, and detect a ransomware attack and resulting data breach within a reasonable time, even though the risk of a data breach or theft was highly likely, especially given Defendant had been on notice for almost a year of the potential for a Conti ransomware attack on its systems. The business acts and practices by Defendant for failure to keep confidential medical or personal data protected, encrypted and without sufficient security to be breached by an adverse third party did not meet all applicable standards of care and vigilance. Thousands of individuals are now prime targets for fraud, extortion, or access to other completely private information that would never have been provided to Defendant if the patients or consumers knew how negligent or reckless Defendant would be in not protecting such deeply personal medical and financial information private.

304. These unlawful and unfair business acts or practices conducted by Defendant have been committed in the past and continue to this day. Defendant has failed to acknowledge the wrongful nature of its actions. Defendant has not timely corrected or publicly issued comprehensive corrective notices to Plaintiffs and the Class Members, and may not have corrected or enacted adequate policies and procedures to protect and preserve the confidentiality of medical and personal identifying information of Plaintiffs and the Class in its possession.

305. As set forth above, Plaintiffs and/or Class Members have been injured in fact and lost money or property as a result of Defendant's unlawful and unfair business practices, having lost control over information about them that has a specific inherent monetary value in that it can be sold, bartered or exchanged.

306. Plaintiffs and Class Members have no other adequate remedy of law in that absent injunctive relief from the Court Defendant is unlikely to fully redress the issues raised by its illegal and unfair business practices. Defendant has not announced any specific changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in the electronic information security systems and/or security practices that permitted the Conti ransomware attack and the Data Breach to occur and go undetected, and thereby prevent further attacks, nor did Defendant provide complete and prompt notice of the circumstances surrounding this breach as required by law.

307. Pursuant to Business & Professions Code section 17203, Plaintiffs seek an order of this Court both for themselves, members of the Class, and for the benefit of the public for injunctive relief in the form of requiring Defendant to correct its illegal conduct, to prevent Defendant from repeating the illegal and wrongful practices as alleged above and protect and preserve confidentiality of Personal Information and Medical Information in Defendant's possession that has been accessed, downloaded, exfiltrated, stolen, and viewed by at least one unauthorized third party because of Defendant's illegal and wrongful practices set forth above.

308. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and/or the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiffs in relation to Plaintiffs' stake in the matter. Because this case is brought for the purposes of enforcing important rights affecting the public interest, Plaintiffs also seek the recovery of attorneys' fees and costs in prosecuting this action against Defendant under Code of Civil Procedure section 1021.5 and other applicable law.

COUNT X
Violations of New York GBL § 349
(on behalf of Plaintiff Migliaccio and the New York Subclass)

309. Plaintiff Migliaccio ("Plaintiff" for the purposes of this Count) re-alleges and incorporates by reference all of the foregoing paragraphs in the Complaint as if fully set forth herein. This count is brought on behalf of the New York Subclass (the "Class" for the purposes of this Count).

310. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a proximate and direct cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify the Plaintiff and Class Members of the Data Breach;

e. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

311. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

312. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

313. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff's and Class Members' rights.

314. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

315. Defendant's conduct is unconscionable, deceptive, and unfair, and is substantially likely to and did mislead consumers such as Plaintiff and the Class acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have been injured because they were not timely notified of the Data Breach causing their Private Information to be comprised.

316. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

317. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid.

318. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: July 15, 2022

Respectfully Submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon (0076050)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Marc E. Dann (0039425)
Brian D. Flick (0081605)
Michael Smith (0097147)
DANNLAW
15000 Madison Avenue
Lakewood, OH 44107
Phone: (216) 373-0539
Fax: (216) 373-0536

notices@dannlaw.com

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
221 West Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (847) 208-4585
gklinger@milberg.com

David K. Lietz (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20115
(866) 252-0878
dlietz@milberg.com

Thomas A. Zimmerman, Jr. (admitted *pro hac vice*)
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Phone: (312) 440-0020
Fax: (312) 440-4180
tom@attorneyzim.com
firm@attorneyzim.com

Nathan D. Prosser (*pro hac vice* forthcoming)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
Fax: (952) 941-2337
nprosser@hjlawfirm.com

WHATLEY KALLAS, LLP
Alan M. Mansfield (*pro hac vice* forthcoming)
16870 W. Bernardo Drive
Suite 400
San Diego, CA 92127
Phone: (619) 308-5034
Fax: (888) 341-5048
amansfield@whatleykallas.com

WHATLEY KALLAS, LLP
Joe R. Whatley, Jr. (*pro hac vice* forthcoming)

Edith M. Kallas (*pro hac vice* forthcoming)
Patrick J. Sheehan (*pro hac vice* forthcoming)
152 W. 57th Street, 41st Floor
New York, NY 10019
Tel: (212) 447-7060
Fax: (800) 922-4851
jwhatley@whatleykallas.com
ekallas@whatleykallas.com
psheehan@whatleykallas.com

APRIL M. STRAUSS, a PC
April M. Strauss (*pro hac vice* forthcoming)
2500 Hospital Drive, Bldg 3
Mountain View, CA 94040
Phone: (650) 281-7081
astrauss@sfaclp.com

DOYLE APC
William J. Doyle (*pro hac vice* forthcoming)
550 West B Street
4th Floor
San Diego, CA 92101
Phone: (619) 736-0000
Fax: (619) 736-1111
bill@doyleapc.com

Attorneys for Plaintiffs and the Proposed Classes

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on July 15, 2022, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Terence R. Coates
Terence R. Coates (0085579)